RECEIVED
CENTRAL FAX CENTER
JUL 12 2007

REMARKS

In the April 12, 2007 Office Action, the Examiner noted that claims 1-8 are pending in the application; rejected claim 8 under 35 U.S.C. § 101; rejected claims 1, 3 and 5-8 under 35 U.S.C. § 102(b) as being anticipated by Choo (U.S. Patent No. 6,981,140); rejected claim 2 under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Iitsuka et al. (U.S. Patent No. 6,463,151); and rejected claim 4 under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Albrecht et al. (U.S. Patent No. 6,510,521). New claims 9 and 10 are added herein. Thus, claims 1-10 are currently pending in the case. The rejections are traversed below.

Rejection under 35 U.S.C. § 101

Claim 8 is rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. The Office Action states that the "claimed subject matter lacks a practical application of a judicial exception" (page 2, last full paragraph). In making the rejection, the Office Action asserted that "the claimed subject matter fails to produce a result that is limited to having real world value rather that a result that may be interpreted as abstract in nature as, for example a computer program" (page 2, last full paragraph). In other words, the Action argues that the result is not tangible. The applicant respectfully disagrees.

Per the USPTO Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility (hereinafter Interim Guidelines), the focus "is not on whether the steps taken to achieve a particular result are useful, tangible and concrete, but rather that the final result achieved by the claimed invention is 'useful, tangible and concrete'" (page 20, lines 9-11). It is respectfully submitted that the features of claim 8 produce useful, concrete and tangible results.

Claim 8 recites "transmitting rule information" (see line 4). Dictionary.com defines "transmit" as:

1. To send or forward, as to a recipient or destination; dispatch; convey.
7. To send a signal by wire, radio, or television waves.

(See http://dictionary.reference.com/browse/transmit, based on the Random House Unabridged Dictionary, © Random House, Inc. 2006). As such, the "transmitting" recited in claim 8 results in sending of a tangible signal containing rule information.

Claim 8 further recites "warning the information management system" (see line 13). A warning is not a mere abstraction. It is a tangible result of the present invention as recited, for

example, in claim 8, informing the information management system that the information was not encrypted in accordance with the rule.

In view of the above, it is respectfully submitted that the rejection is overcome.

Rejection under 35 U.S.C. § 102

Claims 1, 3 and 5-8 are rejected under 35 U.S.C. § 102(b) as being anticipated by Choo (U.S. Patent No. 6,981,140).

Claim 1 recites "an encryption rule storing portion that stores rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret" (lines 5-7). It is respectfully submitted that Choo fails to disclose this feature.

Page 4 of the Office Action states that the security policy database 602 in Fig. 6 of Choo "inherently stores an encryption rule", citing column 11, lines 3-6. The cited portion of Choo discusses "a security policy, comprising a predetermined set of rules for dealing with data packets, is stored in a security policy database 605 and is accessible by the internet protocol security stack 510" (column 11, lines 3-6). However, claim 1 recites that an encryption rule is stored for *each secret level*. Choo is completely silent as to this feature. In fact, Choo describes that user applications and processes "depicted as residing within memory compartment 603 are all processes and/or files and/or data having the *same level of security*" (column 10, lines 54-57).

Claim 1 also recites "a monitoring portion that monitors whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system" (lines 14-16). It is respectfully submitted that Choo also fails to disclose this feature.

Pages 4 and 5 of the Office Action contend that column 10, line 65 through column 11, line 3, column 13, lines 14-20 and Fig. 10 disclose the above feature, stating that "the internet protocol security stack 510 in Fig. 6 is inherently the monitoring portion for monitoring whether the encrypted data received is processed according to the rule/policy prior to transmission." Choo discusses sending data packets to be transmitted to an internet protocol security stack. (See column 10, lines 65-66) "Every data packet to be transmitted must, in order to conform with the internet protocol security protocol, be checked by the internet protocol security stack 510 against a security policy database associated with key database 602" (column 10, line 66 through column 11, line 3, of Choo). "If it is determined that the received data packet is to be

encrypted, then in step 1030, the data packet is encrypted and, in step 1040, returned to the protocol stack via port 509" (column 13, lines 17-20, of Choo).

However, Choo does not monitor whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the *process information* received from the information management system. Per the above, in Choo, each packet is simply checked against a security policy database.

Claim 1 further recites "a warning portion that warns the information management system that was found to encrypt information not in accordance with the rule by the monitoring portion to do encryption of information in accordance with the rule" (lines 17-19). It is respectfully submitted that Choo further fails to disclose this feature.

Page 5 of the Office Action states that the internet protocol security stack in Choo is "equivalent to a warning portion", warning "'an Internet Key Exchange (IKE) block 604, in fig. 6' which resides in the user memory (i.e., information management system) that the encrypted information found is not in accordance with the rule." The Applicant respectfully points out that "user memory" does not, in and of itself, comprise an information management system. See, for example, page 8, line 24 through page 9, line 20 and Fig. 1, of the application.

Further, an IKE block is not "warned". Upon determining that a security association has not been received for transferring a particular block, the internet protocol security stack described in Choo "instructs an Internet Key Exchange (IKE) block 604 to initiate a negotiation procedure with a corresponding respective internet keying agent associated with the remote host across a LAN/WAN 605" (see column 11, lines 6-13). In other words, when no security association is received, a remote internet keying agent is contacted. As such, Choo does not disclose warning an information management system found not to encrypt information in accordance with a rule to do encryption of information in accordance with said rule. Thus, Choo fails to anticipate claim 1 under 35 U.S.C. § 102(b).

Claim 3 depends from claim 1 and adds further limitations thereto. Thus, the arguments above with respect to claim 1 also apply to claim 3.

Claim 5 recites a classification secret level storing portion that stores classification of information managed by the information management system for each classification in connection with the secret level and a process information transmitting portion that transmits process information that indicates the encryption process performed by the encrypting portion to the encryption support system so as to receive a check whether or not the encryption of the

information was performed in accordance with the rule. Thus, claim 5 also patentably distinguishes over Choo.

Claim 6 recites an encryption rule storing portion that stores rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret, a monitoring portion that monitors whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system, and a warning portion that warns the information management system that was found to encrypt information not in accordance with the rule by the monitoring portion to do encryption of information in accordance with the rule. Thus, claim 6 also patentably distinguishes over Choo.

Claim 7 depends from claim 6 and adds further limitations thereto.

Claim 8 recites transmitting rule information that indicates an encryption rule of the information for each secret level that is a level of wanting to keep information secret and encryption data that is necessary for encrypting information in accordance with the rule to the information management system, monitoring whether or not the encryption of information is performed in accordance with the rule by the information management system on the basis of the process information received from the information management system, and warning the information management system that was found to encrypt information not in accordance with the rule by the monitoring means to do encryption of information in accordance with the rule. Thus, claim 8 also patentably distinguishes over Choo.

In view of the above, it is respectfully submitted that the rejection is overcome.

Rejections under 35 U.S.C. § 103

Claim 2 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Iitsuka et al. (U.S. Patent No. 6,463,151).

Claim 2 depends from claim 1 and adds further limitations thereto. Thus, the arguments above pertaining to claim 1 also apply to claim 2 with respect to Choo. Iitsuka et al. also fails to teach the above features. Thus, Choo and Iitsuka et al., both individually and in combination, fail to render claim 2 unpatentable under 35 U.S.C. § 103(a).

In view of the above, it is respectfully submitted that the rejection is overcome.

Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Choo in view of Albrecht et al. (U.S. Patent No. 6,510,521).

Claim 4 depends from claim 1 and adds further limitations thereto. Thus, the arguments above pertaining to claim 1 also apply to claim 4 with respect to Choo. Albrecht et al. also fails to teach the above features. Thus, Choo and Albrecht et al., both individually and in combination, fail to render claim 4 unpatentable under 35 U.S.C. § 103(a).

In view of the above, it is respectfully submitted that the rejection is overcome.

New Claims

New claims 9 and 10 are added herein. Claim 9 recites a method comprising:

> monitoring whether data is encrypted in accordance with a predetermined encryption rule for a security level; and
> producing a warning if the data is not encrypted in accordance with the encryption rule

Choo does not disclose producing a warning if data is not encrypted in accordance with an encryption rule. Iitsuka et al. and Albrecht et al. do not teach these features.

Claim 10 recites a method comprising:

> monitoring whether an information management system encrypts data in accordance with an encryption rule associated with a security level of the information management system; and
> warning the information management system if the data is not encrypted in accordance with the encryption rule.

Choo fails to disclose an information management system. See, for example, page 8, line 24 through page 9, line 20 and Fig. 1, of the application. Further, as demonstrated above, Choo does not disclose warning an information management system if data is not encrypted in accordance with an encryption rule. Iitsuka et al. and Albrecht et al. also fail to teach these features. Thus, it is respectfully submitted that claims 9 and 10 patentably distinguish over the cited art.

Notice of References Cited

The Applicant respectfully points out that Iitsuka et al. is not listed in the Notice of References Cited form that was attached to the outstanding Office Action.

Summary

In accordance with the foregoing, new claims 9 and 10 are added. Therefore, claims 1-10 are pending and under consideration.

Serial No. 10/763,275

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 7-12-2007

By: _____
Michael A. Leonard II
Registration No. 60,180

1201 New York Avenue, NW, 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence is being transmitted via facsimile to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
on 12, 2007
STAAS & HALSEY
By: _____
Date: 7/12/07